Remarks/Arguments:

Applicants' disclosure is directed to a method of enabling access to a data structure. The method includes designating identification of users with respective sections of the data structure and enabling access to the respective sections to users corresponding to the designated identification responsive to the identification of the users being designated with the respective sections of the data structure. An example of the identification is an e-mail address.

Claims 1-18 stand rejected under 35 U.S.C. § 103(a) as obvious over Bott, *Special Editions Using Microsoft Office 2000* (hereinafter "Bott") and Sweet et al. (U.S. Pub. No. 2002/0031230). It is respectfully submitted, however, that the claims are patentable over the art of record for the reasons set forth below.

Applicants' invention, as recited by claim 1, includes a feature which is neither disclosed nor suggested by the art of record, namely:

...designating identification of users with respective sections of the data structure...

...enabling access to the respective sections to users corresponding to the designated identification responsive to designating the identification of the users with the respective sections of the data structure.

This feature is found in the originally filed application at page 4, lines 1-3. No new matter has been added.

Bott discloses different features of Microsoft Excel related to protecting worksheets. The disclosed features include, for example, password protecting workbooks/worksheets, locking cells, sharing workbooks and tracking users' changes to worksheets within the shared workbook. See Bott at pages 592-598.

Sweet discloses granting different people access to different sections of a document. In the embodiment described in Sweet, each different section of the document is designated as a separate data object included within a higher-level data object. See Sweet at paragraph 0138. The data objects are each encrypted "by creating a set of access permission credentials that are selectively assigned to various embedded objects of the data object" (e.g., using the CKM X9.69 ANSI standard). In this way, each object can only be decrypted by a person with access permission to the object. Each user is also given a "security profile in the form of a valid hardware of software token." The security profile includes access permission for the particular

data object(s) he or she needs access permission for. Once a user is in possession of the security profile, that user is "automatically authorized to decrypt the encrypted data upon request for access." See Sweet at paragraphs 0141-0142. Part of the data included in each security file is a user ID. See Sweet at paragraph 155. The Examiner argues that Applicants' user ID is an e-mail address.

The Examiner admits that Bott does not disclose "individualized protection of portions of the spreadsheet by password." However, the Examiner argues that it "would have been obvious to one of ordinary skill in the art at the time of invention to modify the spreadsheet password protections of Bott with the idealized access permission of Sweet in order to 'provide a good one-to-many solution to accessing parts of an information repository.'" See Office Action at paragraph 5 and Sweet at paragraph 0006. The combination of Bott and Sweet would not, however, enable "access to the respective sections to users corresponding to the designated identification responsive to the identification of the user being designated with the respective sections of the data structures," as required.

In particular, to enable access in Sweet, the data is encrypted, a security profile is created which enables the user to decrypt the data, the security profile is distributed to the user, and the user requests access to the data. If password protection were somehow incorporated into Sweet's method, it would only serve to add additional steps (e.g., once the user receives the security profile, the user must also enter the password to access the data). In the example scenario, access would be granted responsive to the user entering the password and not responsive to any associations being made between identifications and respective sections of a data structure, as required.

It should also be noted that while a user ID is incorporated into the security profile in Sweet, Sweet does not disclose that the inclusion of a user ID enables access to anything. Thus, even if Sweet's step of including a user ID in the security profile were read as designating identification of users with respective sections of the data structure, Sweet's method still would not enable "access...responsive to the identification of the users being designated with the respective sections of the data structures," as required (emphasis added).

Accordingly, for the reasons provided above, claim 1 is patentable over the art of record.

Claim 18, while not identical to claim 1, includes features similar to claim 1. Accordingly, claim 18 is also patentable over the art of record for the reasons set forth above.

Claims 2-11 include all features of claim 1 from which they depend. Thus, claims 2-11 are also patentable over the art of record for the reasons set forth above.

Applicants' invention, as recited by claim 12, includes a feature which is neither disclosed nor suggested by the art of record, namely:

> ...the authorization being provided by designating an identification of the user with the portion of the sections in the data structure....

In an exemplary embodiment described in Applicants' specification, this means that by designating the identification with the portion of the sections the user corresponding to the identification is granted access to that portion of the sections. By way of example, a user may be provided with a data sheet which includes all of the data the user is working with. The user may also be provided with an associating sheet. The associating sheet may, for example, have a two columns. One of the columns may be for entering identifications. The other column may include data that associates the cells in the column for entering identifications with respective rows in the data sheet. In this example, the user grants access to users associated with the identifications by entering the identifications in respective cells in the column for entering identifications. This feature is described, for example, in Applicants' specification, e.g., at page 5, lines 13-16.

Once again, to enable a user to access a portion of a document, the alleged combination of Bott and Sweet would enable access by encrypting the data, creating a security profile, distributing, receiving the security profile, requesting access to the data and then entering a password to access the data. In Applicants' claim 12, on the other hand, the user is granted access to a portion of the plurality of sections by designating the user's identification with the portion of the sections. Accordingly, neither Bott, nor Sweet, nor their combination, disclose this feature of Applicants' claim 12.

Accordingly, for the reasons provided above, claim 12 is patentable over the art of record.

Claims 13-17 include all features of claim 12 from which they depend. Accordingly, claims 13-17 are also patentable over the art of record for the reasons set forth above.

Claim 19 is newly added and is supported by the originally filed application, e.g., at page 5, lines 22-30 and FIG. 5.

Applicants' invention, as recited by claim 19, includes a feature which is neither disclosed nor suggested by the art of record, namely:

> ...enabling a first user to view data contained in only the first section of the data structure by entering a first identification associated with the first user in the first cell...
>
> ...enabling a second user to view data contained in only the second section of the data structure by entering a second identification associated with the second user in the second cell.

As described above, in Sweet, a user ID is included in the security profiles. However, no user is enabled to view data contained in a section of the data structure based on the inclusion of the user ID. Moreover, neither Bott nor Sweet disclose enabling access simply by entering an identification in a cell of a data structure.

Accordingly, for the reasons provided above, claim 19 is also patentable over the art of record.

Claim 18 has been amended and is now fully compliant with 35 U.S.C. § 101. Thus, Applicants respectfully request that the Examiner withdraw the § 101 rejection of claim 18.

In view of the amendments and arguments set forth above, the above-identified application is in condition for allowance which action is respectfully requested.

Respectfully submitted,

Lawrence E. Ashery, Reg. No. 34,515
Attorney for Applicants

DK/nm

Dated: August 13, 2008

P.O. Box 980
Valley Forge, PA 19482
(610) 407-0700

NM318785